Europ. J. Combinatorics (1999) **20**, 589–603
Article No. eujc.1999.0306
Available online at http://www.idealibrary.com on IDEAL®

A Family of d-dimensional Dual Hyperovals in $PG(2d+1, 2)$

SATOSHI YOSHIARA

With the affine part of an oval we associate a family of d-subspaces of $PG(2d+1, 2)$ which can be thought of as a higher dimensional analogue of a hyperoval. The isomorphisms among such families together with their automorphisms are determined when they come from translation ovals.

1. INTRODUCTION

A family $\mathcal{S}$ of d-(projective) dimensional subspaces of $PG(m, q)$ is called a *d-dimensional dual arc* if the following four conditions hold:

(a) Any three distinct members of $\mathcal{S}$ intersect trivially.
(b) $X \cap Y$ is a projective point for every distinct members X, Y of $\mathcal{S}$.
(c) For each $X \in \mathcal{S}$, the projective points $X \cap Y$ ($Y \in \mathcal{S}, Y \neq X$) span X.
(d) The members of $\mathcal{S}$ span $PG(m, q)$.

Conditions (a) and (b) give the following upper bound for $|\mathcal{S}|$:

$$|S| \leq 1 + \frac{q^{d+1} - 1}{q - 1} = q^d + q^{d-1} + \cdots + q + 2.$$

A d-dimensional dual arc $\mathcal{S}$ in $PG(m, q)$ is called a *dual hyperoval* if $|\mathcal{S}|$ attains this upper bound: $|\mathcal{S}| = q^d + q^{d-1} + \cdots + q + 2$.

If $|\mathcal{S}| = q^d + q^{d-1} + \cdots + q + 2$, then every point on a member of $\mathcal{S}$ is the intersection of two distinct members of $\mathcal{S}$, and hence the condition (c) is automatically satisfied. Thus if we have a family $\mathcal{S}$ of d-dimensional subspaces of $PG(m, q)$ with the conditions (a), (b) and $|\mathcal{S}| = q^d + q^{d-1} + \cdots + q + 2$, then $\mathcal{S}$ is a d-dimensional dual hyperoval in $\langle \mathcal{S} \rangle \cong PG(m', q)$. As $\mathcal{S}$ contains at least two members (which intersect at a projective point), we have $m' \geq 2d$.

It is immediate to see that a 1-dimensional dual hyperoval in $PG(m, q)$ exists only when $m = 2$, and that the notion of 1-dimensional dual hyperovals coincides with the usual dual hyperoval in $PG(2, q)$. This gives the reason why we use the terminology 'hyperoval'.

The concept of dual arcs is a generalization of certain family of planes in $PG(5, q)$ constructed by the author to obtain an infinite family of extended generalized quadrangles [7, 8]. During that work, the author noticed that one of such families in $PG(5, 4)$ can be enlarged to a dual hyperoval $\mathcal{M}$ in $PG(5, 4)$. (It was alluded to in the preliminary report for the conference Combinatorics '96 in Assisi.) The dual hyperoval $\mathcal{M}$ has some interesting properties: there is a Hermitian form on $PG(5, 4)$ with respect to which every member of $\mathcal{M}$ is maximal totally isotropic: the subgroup of $SU_6(4)$ stabilizing $\mathcal{M}$ is isomorphic to the non-split triple cover of the Mathieu group M_{22}, which induces on the 22 planes $\mathcal{M}$ the usual triply transitive permutation representation of M_{22}. A compact but explicit description of $\mathcal{M}$ is given in [1, p.39, unitary].

The dual hyperoval $\mathcal{M}$ is characterized by Del Fra [3, Theorem 4] as a 2-dimensional dual hyperoval in $PG(5, 4)$ having the property that $\dim(X \cap \langle Y, Z \rangle) = 1$ for every distinct three members X, Y, Z. Huybrechts and Pasini [4] showed that if $\mathcal{S}$ is a dual hyperoval in $PG(m, q)$ ($m > 2$) with the automorphism group acting doubly transitively on its members then $q = 2$, or $\mathcal{S} \cong \mathcal{M}$, or the automorphism group is a 1-dimensional affine group.

0195–6698/99/060489 + 15 $30.00/0

This leads our interest to the construction of dual hyperovals in $PG(m, 2)$ with large symmetry. Recently one infinite family of d-dimensional dual hyperovals was found by Cooperstein and Thas [2]. They constructed d-dimensional dual hyperovals in $PG(2d, 2)$ for every d. Such a dual hyperoval is characterized as the d-dimensional dual hyperoval $\mathcal{S}$ in $PG(2d, 2)$ such that the complement of the union of members in $\mathcal{S}$ forms a $(d-1)$-subspace. In fact, Del Fra [3, Proposition 3.1] shows that every d-dimensional dual hyperoval in $PG(2d, 2)$ satisfies the latter condition, and belongs to the family of Cooperstein and Thas.

In this paper, with each 'affine part' $\mathcal{C}$ of an oval in $PG(2, q)$ (for the precise definition see Section 2), $q = 2^e$ a power of 2, and with every natural number m with $1 \leq m \leq e-1$ coprime to e, we associate a d-dimensional dual hyperoval $\mathcal{S}_m(\mathcal{C})$ embedded in $PG(2d+1, 2)$ (Lemma 1). It is a d-dimensional dual hyperoval in either $PG(2d+1, 2)$ or $PG(2d, 2)$. For $\mathcal{C} = \mathcal{C}_h = \{(t, t^{2^h}) | t \in GF(q)\}$ with h prime to m, the dual hyperoval $\mathcal{S}_m^h := \mathcal{S}_m(\mathcal{C}_h)$ is called a *translation dual hyperoval*, because it admits an affine group $A\Gamma L_1(q)$ acting doubly transitively on $\mathcal{S}_m^h$ (Section 4). The dimension of the space $\langle \mathcal{S}_m^h \rangle$ is $2e-1$ if $m + h \neq e$, or $2(e-1)$ if $m + h = e$ (Proposition 3). Thus $\mathcal{S}_m^h$'s form a new infinite family of d-dimensional dual hyperovals in $PG(2d+1, 2)$, with $d = e-1$, unless $m + h = e$. (The dual hyperoval $\mathcal{S}_m^{e-m}$ spans $PG(2d, 2)$ and hence it belongs to the family of Cooperstein and Thas.) The full automorphism group of $\mathcal{S}_m^h$ is calculated (Proposition 7) and the isomorphisms among $\mathcal{S}_m^h$'s are completely determined (Proposition 11). While group theoretic method is useful to analyze automorphism groups and isomorphisms in higher dimensional cases, the smaller dimensional cases seem require more explict consideration on functional equations associated with each auto/isomorphism. These equations are investigated in the last two sections with certain generality.

2. A Construction

Let $q = 2^e$ and consider the q element field $GF(q)$ as an e-dimensional vector space over $GF(2)$. The set $V := GF(q) \oplus GF(q)$ of pairs (x, y) $(x, y \in GF(q))$ has the structure of a $2e$-space over $GF(2)$ under entrywise addition. Denote the Galois group $Gal(GF(q)/GF(2))$ by $Gal(q)$, and let $\sigma : x \mapsto x^2$ be a generator of $Gal(q)$.

Fix an integer m coprime to e with $1 \leq m \leq e-1$. Then the map $\sigma^m : x \mapsto x^{2^m}$ is a generator of $Gal(q)$. The map $x \mapsto x^{2^m-1}$ is a bijection on $GF(q)^\times$, since for $x, y \in GF(q)^\times$, the condition $x^{2^m-1} = y^{2^m-1}$ implies that $(x^{-1}y)^{\sigma^m} = x^{-1}y$, and hence $x^{-1}y = 1$, the unique nonzero element of the field which is fixed under $\langle \sigma^m \rangle = Gal(q)$. The unique element $y \in GF(q)^\times$ with $y^{2^m-1} = x$ will be denoted $x^{1/(2^m-1)}$.

For $(a, b) \in V$, define an e-subspace $X(a, b)$ of V by

$$X(a, b) := \{(x, ax^{2^m} + bx) \mid x \in GF(q)\}.$$

The intersection of $X(a, b)$ and $X(c, d)$ contains a nonzero vector $(x, ax^{2^m} + bx) = (x, cx^{2^m} + dx)$ iff $x \neq 0$ and $(a+c)x^{2^m} = (b+d)x$. Thus $X(a, b) \cap X(c, d)$ is either a projective point or the empty (projective) set. The former occurs iff $a \neq c$ and $b \neq d$. In this case, the above x is given by $((b+d)/(a+c))^{1/(2^m-1)}$.

Choose a set $\mathcal{C}$ of nonzero vectors of V such that

(i) $a \neq c$ and $b \neq d$ for $(a, b) \neq (c, d) \in \mathcal{C}$,
(ii) no three distinct vectors of $\mathcal{C}$ are collinear,
(iii) $|\mathcal{C}| = q$.

Embedding the affine plane V into the projective plane $PG(2, q) = V \cup \{l_\infty\}$, where l_∞ is a line at infinity, we have an oval $\mathcal{C} \cup \{\infty\}$ with a point ∞ on l_∞ from such a set $\mathcal{C}$. Conversely, every

oval in $PG(2, q)$ with q even can be written as $\{(1, t, F(t))|t \in GF(q)\} \cup \{\infty\}$ $(\infty = (0, 0, 1))$ for a permutation polynomial $F(t)$ with some conditions: so $\mathcal{C} = \{(t, F(t)) \mid t \in GF(q)\}$ satisfies the conditions (i)–(iii). Hence there are lots of ways of choosing a set $\mathcal{C}$ with (i)–(iii). In later sections, we mainly concentrate on $\mathcal{C}$ obtained from translation ovals: that is,

$$\mathcal{C}_h := \{(t, t^{2^h})|t \in GF(q)\}, \text{ for } h, 1 \le h \le e-1, \text{ prime to } e.$$

For a set $\mathcal{C}$ of V with conditions (i)–(iii) above, let $\mathcal{S}_m(\mathcal{C})$ be the family of e-subspaces $X(a, b)$, where (a, b) ranges over $\mathcal{C}$. Condition (i) implies that any two distinct subspaces of $\mathcal{S}$ intersect exactly at a projective point, and hence $\mathcal{S}_m(\mathcal{C})$ satisfies condition (b) in the definiton of the dual arc.

Condition (ii) implies that for three distinct vectors (a_i, b_i) $(i = 1, 2, 3)$ of $\mathcal{C}$, the three slopes $(b_i + b_j)/(a_i + a_j)$ $(1 \le i \ne j \le 3)$ of the lines through two of them are mutually distinct. It follows from the above remark about $X(a, b) \cap X(c, d)$ that three distinct subspaces $X(a_i, b_i)$ $(i = 1, 2, 3)$ intersect trivially. Thus $\mathcal{S}_m(\mathcal{C})$ satisfies condition (a) in the definiton of the dual arc.

By (iii), $|\mathcal{S}_m(\mathcal{C})| = q$, which coincides with $(2^{e-1} + 2^{e-2} + \cdots + 1) + 1 = 2^e - 1 + 1$. Since the projective dimension of each $X(a, b)$ of $\mathcal{S}_m(\mathcal{C})$ is $e - 1$, this implies that the upper bound for the cardinality of $(e - 1)$-dimensional dual arc is satisfied. Hence we verified:

LEMMA 1. *The family $\mathcal{S}_m(\mathcal{C})$ is an $(e - 1)$-dimensional dual hyperoval in $\langle \mathcal{S}_m(\mathcal{C}) \rangle$.*

3. DIMENSION OF THE WHOLE SPACE

In the following, the dimension always means the projective dimension, unless otherwise stated. We have $\dim V = 2e - 1$ and $\dim \langle X, Y \rangle = 2(e - 1)$ for two distinct members X, Y of $\mathcal{S}_m(\mathcal{C})$, as $dim(X \cap Y) = 0$. Thus $\langle \mathcal{S}_m(\mathcal{C}) \rangle$ coincides with V or a hyperplane of V.

We now concentrate on the dual hyperoval $\mathcal{S}_m(C_h)$ constructed from $\mathcal{C}_h := \{(t, t^{2^h})|t \in GF(q)\}$ for h, $1 \le h \le e - 1$, prime to e. We refer to $\mathcal{S}_m(C_h)$ as a *translation dual hyperoval*. We write $\mathcal{S}_m^h := \mathcal{S}_m(C_h)$ for short, and set $X(t) := X(t, t^{2^h}) = \{(x, x^{2^m} t + x t^{2^h})|x \in GF(q)\}$. Moreover $Tr = Tr_{GF(q)/GF(2)}$ denotes the absolute trace from $GF(q)$ onto $GF(2)$.

LEMMA 2. *Let m, h be integers with $1 \le m, h \le e$ and prime to e. If $m + h \ne e$, every element of $GF(q)$ with $q = 2^e$ can be written as $x^{2^m} t + x t^{2^h}$ for some $x, t \in GF(q)$. If $m + h = e$, the set $\{x^{2^m} t + x t^{2^h} | x, t \in GF(q)\}$ coincides with $GF(q)_0 := \{y \in GF(q)|Tr(y) = 0\}$.*

PROOF. Clearly $0 = x^{2^m} t + x t^{2^h}$ for $x = 0$. Let y be any element of $GF(q)^\times$. There are $x, t \in GF(q)^\times$ with $y = x^{2^m} t + x t^{2^h}$ if and only if the polynomial $\lambda^{2^h} + x^{(2^m-1)}\lambda + (y/x)$ has a solution t in $GF(q)^\times$ for some $x \in GF(q)^\times$. In general, a polynomial $\lambda^{2^h} + a\lambda + b$ over $GF(q)$ with $a \ne 0$ can be written as $c^{2^h}((\lambda/c)^{2^h} + (\lambda/c) + b/c^{2^h})$, where $c = a^{1/(2^h-1)}$ (as $(h, e) = 1$, c is well defined), and hence the above polynomial is reducible over $GF(q)$ if and only if $Tr(b/a^{2^h/(2^h-1)}) = 0$. As $x \cdot (x^{2^m-1})^{2^h/(2^h-1)} = x^{(2^{m+h}-1)/(2^m-1)}$, we conclude $y = x^{2^m} t + x t^{2^h}$ for some $x, t \in GF(q)^\times$ if and only if $Tr(y/x^{(2^{m+h}-1)/(2^m-1)}) = 0$ for some $x \in GF(q)^\times$.

Assume $m + h \ne e$ and suppose $Tr(y/x^{(2^{m+h}-1)/(2^m-1)}) = 1$ for every $x \in GF(q)^\times$. Taking a generator ζ of $GF(q)^\times$ and setting $\delta := \zeta^{(2^{m+h}-1)/(2^m-1)}$, we have $Tr(y\delta^i) = 1$ for every $i = 0, \ldots, l - 1$, where l is the order of δ in $GF(q)^\times$. Then l is an odd number and $\delta \ne 1$, as $m + h \ne e$. We have $\sum_{i=0}^{l-1} \delta^i = (1 + \delta^l)/(1 + \delta) = 0$, and so $Tr\left(\sum_{i=0}^{l-1}(x\delta^i)\right) = Tr\left(x\left(\sum_{i=0}^{l-1}\delta^i\right)\right) = Tr(0) = 0$. On the other hand, this trace is equal to $l \cdot 1 = 1$, as l is odd. This

contradiction shows that there is $x \in GF(q)^\times$ with $Tr(y/x^{(2^{m+h}-1)/(2^m-1)}) = 0$, and hence the former claim is established. If $m+h=e$, then $(x^{2^m}t)^{2^h} = xt^{2^h}$ and $Tr(x^{2^m}t + xt^{2^h}) = Tr(x^{2^m}t) + Tr(xt^{2^h}) = 2Tr(xt^{2^h}) = 0$. Conversely every element of $GF(q)_0$ can be written as $x^{2^m}+x$, since $x \mapsto x^{2^m}$ is a generator of $Gal(q)$. This shows the latter claim. □

PROPOSITION 3. *If $m+h \neq e$ (resp. $m+h=e$), the family $\mathcal{S}_m^h$ is an $(e-1)$-dimensional dual hyperoval in $V \cong PG(2e-1,2)$ (resp. $W := \{(x,y)|x,y \in GF(q), Tr(y)=0\} \cong PG(2e-2,2)$).*

PROOF. As $x \mapsto x^{2^m}$ is a generator of $Gal(q)$, we have $GF(q)_0 = \{y^{2^m}+y | y \in GF(q)\}$. Thus the $2(e-1)$-space $\langle X(0), X(1)\rangle$ consisting of vectors $(x,0)$, $(y, y^{2^m}+y)$ and $(x,0)+(y,y^{2^m}+y) = (x+y, y^{2^m}+y)$ for $x,y \in GF(q)$ coincides with the hyperplane W of V.

Each point of $X(t)$ is of the form $(x, x^{2^m}t + xt^{2^h})$ for some $x \in GF(q)$. If $m+h \neq e$, there are some $x,t \in GF(q)$ with $Tr(x^{2^m}t + xt^{2^h}) = 1$ by the former claim of Lemma 2. The corresponding point is not contained in W. Thus $\langle \mathcal{S}_m \rangle = V$ if $m+h \neq e$. If $m+h=e$, each point of $X(t)$ lies in W for every $t \in GF(q)$ by the latter claim of Lemma 2. Thus $\langle \mathcal{S}_m \rangle = W$ if $m+h=e$. □

4. AUTOMORPHISM GROUPS

DEFINITION. For a d-dimensional dual arc $\mathcal{S}$ in $PG(m,q)$, the automorphism group $Aut(\mathcal{S})$ is defined to be the group of automorphisms of $PG(m,q)$ which send each member of $\mathcal{S}$ to one of $\mathcal{S}$.

The following lemma holds for any dual hyperoval over $GF(2)$, which yields many dual hyperovals as 'subhyperovals' fixed by automorphisms.

LEMMA 4. *Let $\mathcal{S}$ be an r-dimensional dual hyperoval $\mathcal{S}$ in $PG(v,q)$. For a nontrivial automorphism σ of $\mathcal{S}$, set $\mathcal{S}^{(\sigma)} := \{X \in \mathcal{S} | X^\sigma = X\}$, $C(\sigma)$ the subspace of projective points in $PG(v,q)$ fixed by σ, and $\mathcal{S}(\sigma) := \{X \cap C(\sigma) \mid X \in \mathcal{S}^{(\sigma)}\}$.*

(1) *The stabilizer of $X \in \mathcal{S}$ in $Aut(\mathcal{S})$ acts faithfully on the projective points of X. In particular, $Aut(\mathcal{S})$ acts faithfully on $\mathcal{S}$.*
(2) *Assume $q=2$. The dimension of $X \cap C(\sigma)$ does not depend on the particular choice of $X \in \mathcal{S}^{(\sigma)}$, say f. If $f \geq 0$, $\mathcal{S}(\sigma)$ forms an f-dimensional dual hyperoval in $\langle \mathcal{S}(\sigma)\rangle$. Furthermore we have $v-r-1 \geq \dim(C(\sigma)) \geq \dim(\langle \mathcal{S}(\sigma)\rangle) \geq 2f$, unless σ induces an involution on $\mathcal{S}$. In the exceptional case, we have $v-r \geq \dim(C(\sigma)) \geq \dim(\langle \mathcal{S}(\sigma)\rangle) \geq 2f$.*

PROOF. (1) If an automorphism σ fixes each point p of X, then σ stabilizes all members of $\mathcal{S}$, as there is a unique member of $\mathcal{S}-\{X\}$ containing p. Then each point on any member of $\mathcal{S}$ is fixed by σ, since it is the intersection of two members of $\mathcal{S}$. As $PG(v,q)$ is generated by $\mathcal{S}$, σ is the identity.

If an automorphism σ fixes every member of $\mathcal{S}$, then it fixes their intersections, and hence $\sigma = 1$ by the claim above.

(2) Take $X \in \mathcal{S}^{(\sigma)}$. For every $Y \in \mathcal{S}^{(\sigma)} - \{X\}$, $X \cap Y \subseteq X \cap C(\sigma)$. Conversely, for every point p of $X \cap C(\sigma)$ there is a unique member Y of $\mathcal{S}$ with $X \cap Y = p$. Since X and p are stabilized by σ, Y is also. Thus there is a bijective correspondence between $\mathcal{S}^{(\sigma)} - \{X\}$ and the points of $X \cap C(\sigma)$. Thus $|X \cap C(\sigma)|$ is constant, and the first claim follows as $q=2$.

Let f be the constant dimension of $X \cap C(\sigma)$, and assume $f \geq 0$. By the above correspondence $|\mathcal{S}(\sigma)| = |\mathcal{S}^{(\sigma)}| = 2^{f+1} = (2^f + \cdots 2 + 1) + 1$. As no three members of $\mathcal{S}$ intersect nontrivially, $\mathcal{S}(\sigma)$ is an f-dimensional dual hyperoval in $\langle \mathcal{S}(\sigma)\rangle$.

As $f \geq 0$, there are at least two distinct members in $\mathcal{S}^{(\sigma)}$. Thus $\dim(\langle \mathcal{S}(\sigma)\rangle) \geq 2f$. On the other hand, as $Aut(\mathcal{S})$ acts faithfully on $\mathcal{S}$ by Lemma 4(1), there is at least one $Y \in \mathcal{S} \setminus \mathcal{S}^{(\sigma)}$. Assume $Y \cap C(\sigma) \neq \emptyset$. Let Z_p be the member of $\mathcal{S} - \{Y\}$ containing a point p of $Y \cap C(\sigma)$. Then $Y^\sigma = Z_p$ as $Y^\sigma \neq Y$. In particular, $Z_p = Y^\sigma = Z_q$ if $Y \cap C(\sigma)$ contains two distinct points p, q. However this implies $p = Z_p \cap Y = Z_q \cap Y = q$, a contradiction. Thus $Y \cap C(\sigma)$ contains at most one point.

Summarizing, either $Y \cap C(\sigma) = \emptyset$ for some $Y \in \mathcal{S} \setminus \mathcal{S}^{(\sigma)}$ or $Y \cap C(\sigma) = Y \cap Y^\sigma$ is a projective point for every $Y \in \mathcal{S} \setminus \mathcal{S}^{(\sigma)}$. In the former (resp. latter) case, we have $v \geq \dim(\langle C(\sigma), Y\rangle) = \dim(C(\sigma)) + \dim(Y) - (-1)$ (resp. $v \geq \dim(\langle C(\sigma), Y\rangle) = \dim(C(\sigma)) + \dim(Y)$) and hence $v - r - 1 \geq \dim(C(\sigma)) \geq \dim(\langle \mathcal{S}(\sigma)\rangle) \geq 2f$ (resp. $v - r \geq \dim(C(\sigma)) \geq \dim(\langle \mathcal{S}(\sigma)\rangle) \geq 2f$). □

Now we consider the automorphism group of the translation dual hyperoval $\mathcal{S}_m^h$. We follow the convention in Sections 2 and 3. When $e = 2$, $m = h = 1$ is the unique possibility and $\mathcal{S}_1^1$ is just an ordinary dual 4-gon. Thus we assume $e \geq 3$.

By Proposition 3, $Aut(\mathcal{S}_m^h) = \{\sigma \in GL(V) | \sigma(\mathcal{S}_m^h) = \mathcal{S}_m^h\}$ for $m+h \neq e$, and $Aut(\mathcal{S}_m^{e-m}) = \{\sigma \in GL(W) | \sigma(\mathcal{S}_m^{e-m}) = \mathcal{S}_m^{e-m}\}$, where $W = \{(x, y) | x, y \in GF(q), Tr(y) = 0\}$. For each $a \in GF(q)$ (resp. $b \in GF(q)^\times$ and $\sigma \in Gal(q)$), let t_a (resp. m_b and f_σ) be the linear transformation on V defined by

$$\begin{aligned}(x, y)t_a &:= (x, x^{2^m} a + x a^{2^h} + y),\\ (x, y)m_b &:= (xb, yb^{(2^{m+h}-1)/(2^h-1)}) \text{ and}\\ (x, y)f_\sigma &:= (x^\sigma, y^\sigma).\end{aligned}$$

The images of a vector $(x, x^{2^m} t + x t^{2^h})$ of $X(t)$ by t_a, m_b and f_σ are

$$\begin{aligned}&(x, x^{2^m}(t + a) + x(t + a)^{2^h}) \in X(t + a)\\ &(xb, (xb)^{2^m}(b^{(2^m-1)/(2^h-1)}t) + (xb)(b^{(2^m-1)/(2^h-1)}t)^{2^h}) \in X(b^{(2^m-1)/(2^h-1)}t),\\ &\text{and } (x^\sigma, (x^\sigma)^{2^m} t^\sigma + x^\sigma (t^\sigma)^{2^h}) \in X(t^\sigma),\end{aligned}$$

respectively. Thus the maps t_a, m_b and f_σ preserve $\mathcal{S}_m^h$, and they lie in $Aut(\mathcal{S}_m^h)$. We refer to t_a for $a \in GF(q)$ (resp. m_b for $b \in GF(q)^\times$ or f_σ for $\sigma \in Gal(q)$) as a *translation* (resp. a *multiplication* or a *field automorphism*) of $\mathcal{S}_m^h$. The group $T := \{t_a | a \in GF(q)\}$ is isomorphic to the additive group $GF(q)$ via $t_a \mapsto a$ and acts regularly on $\mathcal{S}_m^h$. The group $M := \{m_b | b \in GF(q)^\times\}$ is isomorphic to the multiplicative group $GF(q)^\times$ via $m_b \mapsto b$ and acts regularly on $\mathcal{S}_m^h \setminus \{X(0)\}$. The group $F := \{f_\sigma | \sigma \in Gal(q)\}$ is isomorphic to $Gal(q)$ via $f_\sigma \mapsto \sigma$ and acts semiregularly on $\mathcal{S}_m^h \setminus \{X(0), X(1)\}$. The subgroup T is normalized by M and F ($m_b^{-1} t_a m_b = t_{ab^{(2^m-1)/(2^h-1)}}$, $f_{(\sigma)^{-1}} t_a f_{(\sigma)} = t_{a^\sigma}$), the group M is normalized by F ($f_{(\sigma)^{-1}} m_b f_{(\sigma)} = m_{b^\sigma}$), and they generate the group $T : (M : F)$ isomorphic to the 1-dimensional semilinear affine group $A\Gamma L_1(q)$ over $GF(q)$. In particular, $Aut(\mathcal{S}_m^h)$ acts doubly transitively on $\mathcal{S}_m^h$ for every m and h.

LEMMA 5. *One of the following holds on the structure of the stabilizer A of $X(0)$ in $Aut(\mathcal{S}_m^h)$:*

(1) $A \cong GL_1(2^e) \cong Z_{2^e-1} : Z_e$.
(2) $A \cong GL_e(2)$, $m + h \neq e$ *and* $e = 3$ *or* 4.
(3) $A \cong GL_e(2)$, $m + h = e = 3$.
(4) $e = 2k$ *and* A *contains a normal subgroup isomorphic to* $GL_2(2^k)$.

PROOF. Let us denote by A the stabilizer of $X(0)$ in $Aut(\mathcal{S}_m^h)$. The group A acts faithfully on $X(0)$ by Lemma 4(1). As m_b and f_σ induce the multiplication $(x,0) \mapsto (xb,0)$ and the field automorphism $(x,0) \mapsto (x^\sigma,0)$ on $X(0)$, respectively, A is isomorphic to a subgroup of $GL_e(2) \cong GL(X(0))$ containing $GF(q)^\times : Gal(q)$ (the normalizer of a Singer cycle). It follows from [6] that a subgroup of $GL_e(2)$ containing a Singer cycle has a normal subgroup isomorphic to $GL_d(2^{e/d})$ for some divisor d of e. (Note that [6] does not depend on any group-theoretic classification theorems.)

Assume first that $d < e$. Then $A \trianglerighteq GL_d(2^{e/d})$ contains an element σ corresponding to the diagonal matrix $diag(1,\ldots,1,\zeta)$, where ζ is a generator of $GF(2^{e/d})^\times$. As σ is an element of odd order $2^{e/d}-1$ (>1) fixing a $(d-1)(e/d)$-(vector) dimensional subspace of $X(0)$ over $GF(2)$, we may apply the first inequality of Lemma 4(2) to $v = 2e-1$ if $m+h \neq e$ (resp. $v = 2e-2$ if $m+h=e$), $r = e-1$ and $f = (d-1)(e/d)-1$. Then we have $e-1 = (2e-1)-(e-1)-1 \geq 2(d-1)(e/d)-2$ in both cases, and hence $d \geq (d-2)e$. As $e > d$, we have $d = 1$ or 2.

When $d = 1$ or $d = 2$, we have case (1) or (4), respectively. Assume $d = e$. Then $A \cong GL_e(2)$. Take an involution σ of A which corresponds to the matrix with (i,j)-entry 1 if $i = j$ or $i = e$, $j = 1$ and 0 otherwise. Since σ fixes an $(e-1)$-(vector) dimensional subspace of $X(0)$, we can apply the second inequality of Lemma 4(2) to $v = 2e-1$ if $m+h \neq e$ ($v = 2e-2$ if $m+h=e$), $r = e-1$ and $f = e-2$. Then we have $v-r = e \geq 2(e-2)$ and so $4 \geq e$ if $m+h \neq e$ (resp. $e-1 \geq 2(e-2)$ and so $3 \geq e$ if $m+h=e$). Cases (2) and (3) arise. □

LEMMA 6. *Case* (4) *in Lemma 5 does not occur.*

PROOF. In this case, $e = 2k$ is even and A contains a subgroup G isomorphic to $GL_2(2^k)$. Via $(x,0) \mapsto x$, we identify $X(0) = \{(x,0) | x \in GF(2^{2k})\}$ with a 2-dimensional vector space $GF(2^{2k})$ over $GF(2^k)$, and let $\{1,\rho\}$ be a basis of $GF(2^{2k})$ over $GF(2^k)$. The action of G on $X(0)$ induces a group $GL_2(2^k)$ of $GF(2^k)$-linear bijections on $GF(2^{2k})$. For an element $g \in G$, we denote by $\bar{g}$ the $GF(2^k)$-linear bijection on $GF(2^{2k}) = X(0)$.

The group G also acts on $\mathcal{S}_m^h$. We denote by $\hat{g}$ the permutation on the index set $GF(2^{2k})$ of the members of $\mathcal{S}_m^h$ induced by $g \in G$: $X(t)g = X((t)\hat{g})$ $(t \in GF(2^{2k}))$. Clearly $(0)\hat{g} = 0$ for every $g \in G$.

Note that $X(t) \cap X(0) = (t^\varepsilon, 0)$ for each $t \in GF(2^e)^\times$, where $\varepsilon := (2^h-1)/(2^m-1)$. Thus $X(t^{1/\varepsilon})$ is the unique member of $\mathcal{S}_m^h - \{X(0)\}$ containing a point $(t,0)$ of $X(0)$ $(t \in GF(2^{2k}))$. Thus if $g \in G$ sends $(t,0)$ to $((t)\bar{g},0)$, then g sends $X(t^{1/\varepsilon})$ to $X(((t)\bar{g})^{1/\varepsilon})$. Thus we obtain the following relation of the two actions of G:

$$(t^{1/\varepsilon})\hat{g} = ((t)\bar{g})^{1/\varepsilon} (t \in GF(2^e), g \in G).$$

Also observe that the map $GF(2^{2k}) \ni x \mapsto x^{2^h-1}$ preserves $GF(2^k)$, as $(h,2k) = 1$, and similary for $x \mapsto x^{2^m-1}$. Thus for $t \in GF(2^{2k})$, we have $t^\varepsilon \in GF(2^k)$ iff $t \in GF(2^k)$.

Let τ be the involution of G sending a point $(a+b\rho,0)$ of $X(0)$ to $(a+b+b\rho,0)$, where $a,b \in GF(2^k)$. Then $(a+b\rho)\bar{\tau} = a+b\rho$ iff $b = 0$. Hence the above formula and the remark show that $X(\alpha)\tau = X(\alpha)$ iff $\alpha \in GF(2^k)$, and $X(\alpha) \cap C_V(\tau) = \{(x, x^{2^m}\alpha + \alpha^{2^h}x) | x \in GF(2^k)\}$. In particular, $X(\alpha) \cap C_V(\tau)$ is of (vector) dimension $k = dim(X(\alpha))/2$, and so $[X(\alpha),\tau] = X(\alpha) \cap C_V(\tau)$. (Recall here the following fundamental facts: if an involution τ acts on a vector space V over $GF(2)$, then the commutator space $[V,\tau] = \{v + v^\tau | v \in V\}$ is contained in the centralizer $C_V(\tau)$, and the additive map $v \mapsto v + v^\tau$ induces the isomorphism $V/C_V(\tau) \cong [V,\tau]$. In particular, $\dim(C_V(\tau)) \geq \dim(V)/2$ and the equality holds iff $C_V(\tau) = [V,\tau]$.)

Assume that $h+m \neq e = 2k$. Then the commutator space $[V,\tau]$ is contained in the hyperplane $W := \langle X(0), X(1)\rangle = \{(x,y)|x,y \in GF(2^{2k}), Tr(y)=0\}$, as τ trivially acts on the 1-dimensional space V/W over $GF(2)$. Assume also that $h+m \neq k$. Then Lemma 2 implies that there are some $x, \alpha \in GF(2^k)$ with $Tr(y)=1$, where $y = x^{2^m}\alpha + \alpha^{2^h}x$. Thus (x,y) lies in $X(\alpha) \cap C_V(\tau) = [X(\alpha),\tau] \leq [V,\tau]$, but is not contained in the hyperplane W, as $Tr(y) \neq 0$, which is a contradiction.

Now consider the remaining case $h+m \equiv 0$ modulo k. The stabilizer A contains a Singer cycle $m_\eta : V \ni (x,y) \mapsto (\eta x, \eta^{(2^{h+m}-1)/(2^m-1)}y) \in V$, where η is a generator of $GF(2^{2k})^\times$ (see the formula for multiplication m_b in this section). Then $z := m_\eta^{2^k+1}$ induces the multiplication by a generator of $GF(2^k)^\times$ on $X(0)$, and hence z is a generator of the center of $G \cong GL_2(2^k)$. By the above formula and our assumption $h+m \equiv 0 \bmod k$, we see $C_V(z) = \{(0,y)|y \in GF(2^{2k})\}$. As z lies in the center of $G = \langle z\rangle \times S$, the subgroup $S \cong SL_2(2^k)$ acts on $C_V(z)$. In particular, the above involution $\tau \in S$ acts on $C_V(z)$, a 2-dimensional space over $GF(2^k)$. As $C_V(\tau)$ has the vector dimension at most $2k+1$ by Lemma 4(2), the action of S on $C_V(z)$ is faithful and irreducible.

If $h+m=e$, then $S \cong SL_2(2^k)$ acts also on the $(2k-1)$-dimensional space $C_V(z) \cap W$ over $GF(2)$, which is impossible. Thus $h+m=k$ and the action of S on $C_V(\tau)$ is the natural action of $SL_2(2^k)$ on $GF(2^k)^2$. In particular, the centralizer $C_V(\tau) \cap C_V(z)$ of the involution τ of $SL_2(2^k)$ is 1-dimensional over $GF(2^k)$, and hence $C_V(\tau) \cap C_V(z) = [C_V(z),\tau]$ by the fundamental property mentioned above.

Since $C_V(\tau) \cap X(0) = \{(x,0)|x \in GF(2^k)\}$ and $C_V(\tau) \cap X(1) = \{(x, x^{2^m}+x)|x \in GF(2^k)\}$ span $\{(x,y)|x,y \in GF(2^k), Tr(y)=0\}$, the centralizer $C_V(\tau)$ contains a $(2k-1)$-dimensional vector space $\{(x,y)|x,y \in GF(2^k), Tr(y)=0\}$. For any $a \in GF(2^{2k})\backslash GF(2^k)$, the subspace of $GF(2^{2k})$ spanned by a and $\{y \in GF(2^k)|Tr(y)=0\}$ does not have the structure of $GF(2^k)$, and therefore we have $C_V(\tau) \cap C_V(z) = [C_V(z),\tau] = \{(0,y)|y \in GF(2^k)\}$. However, this implies again that $[V,\tau]$ contains an element $(0,y)$ with $Tr(y)=1$, which is outside of the hyperplane W, a contradiction. □

The dual hyperovals for which the full automorphism groups have not yet been determined in Lemmas 5 and 6 are: $\mathcal{S}_1^1$ and $\mathcal{S}_2^2$ for $e=3$ and $m+h \neq 3$; $\mathcal{S}_2^1$ and $\mathcal{S}_1^2$ for $e=3$ and $m+h=3$; and $\mathcal{S}_1^1$ and $\mathcal{S}_3^3$ for $e=4$ and $m+h \neq 4$. In Section 5, we will see that $\mathcal{S}_1^1 \cong \mathcal{S}_2^2$, $\mathcal{S}_2^1 \cong \mathcal{S}_1^2$ if $e=3$, and $\mathcal{S}_1^1 \cong \mathcal{S}_3^3$ if $e=4$. The automorphism groups of these three remaining cases will be calculated in Sections 6 and 7, observing functional equations determined by automorphisms. Summarizing the results there and the lemmas above, we have the following.

PROPOSITION 7. *Let $\mathcal{S}_m^h$ be a translation dual hyperoval in $PG(2e-1,2)$ if $m+h \neq e$ (resp. $PG(2e-2,2)$ if $m+h=e$), where e, m, h are integers with $e \geq 3$, $1 \leq m, h \leq e-1$ and m, h being coprime to e. Then $Aut(\mathcal{S}_m^h) = A\Gamma L_1(2^e)$ except when $e=3$ and $(m,h)=(1,1)$ or $(2,2)$. In the exceptional case, $\mathcal{S}_1^1 \cong \mathcal{S}_2^2$ and $Aut(\mathcal{S}_1^1) = 2^3 : GL_3(2)$.*

5. ISOMORPHISMS AMONG TRANSLATION DUAL HYPEROVALS

Let m, n and h, k be integers with $1 \leq m, n, h, k \leq e$ prime to e. For $(e-1)$-dimensional dual hyperovals $\mathcal{S}_m^h$ and $\mathcal{S}_n^k$ in $PG(2e-1,2)$ ($PG(2(e-1),2)$ if $m+h=e=n+k$), we consider when they are isomorphic. Here $\mathcal{S}_m^h$ and $\mathcal{S}_n^k$ are called *isomorphic* if there is a linear bijection $\tau \in GL(V)$ (or $GL(W)$ if $m+h=n+k=e$, where $W = GF(q) \oplus GF(q)_0$) with $(\mathcal{S}_m^h)\tau = \mathcal{S}_n^k$. We put suffices (e.g. $X_m^h(t)$) to distinguish the members of $\mathcal{S}_m^h$ from those of $\mathcal{S}_n^k$.

PROPOSITION 8. *For $1 \leq m, n \leq e-1$ coprime to e, $\mathcal{S}_m^{e-m}$ is isomorphic to $\mathcal{S}_n^{e-n}$.*

PROOF. As $(n,e)=(m,e)=1$, every element of $GF(q)_0$ can be written as $z^{2^m}+z$ for some $z\in GF(q)$. We have $z^{2^m}+z=(z')^{2^m}+z'$ if and only if $z'=z$ or $z'=z+1$. Thus the map $GF(q)_0\ni z^{2^m}+z\mapsto z^{2^n}+z\in GF(q)_0$ is well defined and a linear bijection. Define $\tau\in GL(W)$ by $\tau(x,z^{2^m}+z):=(x,z^{2^n}+z)$.

Then τ sends a typical vector $(x,z^{2^m}+z)$ of $X_m^{e-m}(t)\in\mathcal{S}_m^{e-m}$, where $z=xt^{2^{e-m}}$, to

$$(x,z^{2^n}+z)=(x,x^{2^n}t^{2^{2e-m+n}}+xt^{2^{e-m}})=(x,x^{2^n}t^{2^{2e-m+n}}+x(t^{2^{e-m+n}})^{2^{e-n}}),$$

which lies in $X_n^{e-n}(t^{2^{e-m+n}})\in\mathcal{S}_n^{e-n}$. Thus τ gives an isomorphism of $\mathcal{S}_m^{e-m}$ with $\mathcal{S}_n^{e-n}$. □

In the following, we assume $m+h\neq e$ and $n+k\neq e$. Since $Aut(\mathcal{S}_n^k)$ contains the group of translations, we may assume that $\tau(X_m^h(0))=X_n^k(0)$. Taking the suitable basis for $X_m^h(0)=\{(x,0)|x\in GF(q)\}=X_n^k(0)$ and those for $\{(0,y)|y\in GF(q)\}$, we represent τ as a matrix of the form $\begin{pmatrix}A&0\\B&C\end{pmatrix}$. The following observation was suggested by Kantor.

LEMMA 9. *If $\mathcal{S}_m^h$ is isomorphic to $\mathcal{S}_n^k$, then there is an isomorphism τ from $\mathcal{S}_m^h$ to $\mathcal{S}_n^k$ preserving $X_m^h(0)=X_n^k(0)$ and sending the group M_m^h of multiplications for $\mathcal{S}_m^h$ to that for $\mathcal{S}_n^k$.*

PROOF. First assume $e\neq 6$. Then there is a prime divisor p of $q-1$ which does not divide 2^j-1 for any $1\leq j\leq e-1$. Since the stabilizers A_m^h and A_n^k of $X_m^h(0)=X_n^k(0)$ respectively in $Aut(\mathcal{S}_m^h)$ and $Aut(\mathcal{S}_n^k)$ are subgroups of $GL_e(2)$, as we remarked in Section 4, the image $\tau(P)$ of the Sylow p-subgroup P of M_m^h (of order the p-part of $q-1$) is a Sylow p-subgroup of A_n^k. By the Sylow theorem, we may assume that τ sends P to the Sylow p-subgroup Q of M_n^k. Then τ sends the centralizer M_m^h of P in A_m^h ($\leq GL_e(2)$) to the centralizer M_n^k of Q in A_n^k.

When $e=6$, we can directly show that $Aut(\mathcal{S}_n^k)$ contains $GL_s(2^{6/s})$ as a normal subgroup for some divisor s of 6 (this also follows from [6]). As Singer cycles of $GL_s(2^{6/s})$ are conjugate to each other, $(M_m^h)\tau$ is conjugate to M_n^k under $Aut(\mathcal{S}_n^k)$. Thus the claim follows in this case also. □

LEMMA 10. *Assume that X is an e-vector dimensional subspace of V invariant under M_m^h such that $X\cap X(\alpha)=\{0\}$ for every member $X(\alpha)$ of $\mathcal{S}_m^h$. Then either $X=\{(0,y)|y\in GF(q)\}$ or possibly $X=\{(x,cx^{(2^{h+m}-1)/(2^h-1)})|x\in GF(q)\}$ for some constant $c\in GF(q)$.*

PROOF. Let (x_i,y_i) $(i=1,\ldots,k)$ be a basis of X over $GF(2)$. If y_i are linearly dependent, $\sum_{j\in J}y_j=0$ for some proper subset J of $\{1,\ldots,k\}$, but this forces $\sum_{j\in J}(x_j,y_j)=\left(\sum_{j\in J}x_j,0\right)\in X\cap X(0)$, contradicting the assumption. Hence y_i $(i=1,\ldots,k)$ form a basis of $GF(q)$, and there is a $GF(2)$-linear map ρ on $GF(q)$ with $(y_i)\rho=x_i$ $(i=1,\ldots,k)$, namely $X=\{((y)\rho,y)|y\in GF(q)\}$.

Since X is invariant under M, setting $\delta:=(2^{m+h}-1)/(2^h-1)$, we have $((y)\rho,y)m_b=(b\cdot(y)\rho,b^\delta y)\in X$, and hence

$$(b^\delta y)\rho=b\cdot(y)\rho$$

for every $b\in GF(q)^\times$ and $y\in GF(q)$. If $\rho=0$, then we have $X=\{(0,y)|y\in GF(q)\}$. Suppose $\rho\neq 0$. Then $(y)\rho\neq 0$ for some $y\in GF(q)$, and the above equation implies that ρ is surjective, and hence bijective. In particular, $(1)\rho\neq 0$. We define a constant c by $(1)\rho:=c^{-1/\delta}$. Setting $\tau=\rho^{-1}$, we then have $b^\delta=(bc^{-1/\delta})\tau$ $(b\in GF(q))$ from the above equation putting $y=1$. Thus $(x)\tau=cx^\delta$ for $x\in GF(q)$ and $X=\{(x,cx^\delta)|x\in GF(q)\}$ in this case. □

PROPOSITION 11. *For integers m, h, n, k between 1 and $e-1$ prime to e with $m+h \neq e$ and $n+k \neq e$, the translation dual hyperoval $\mathcal{S}_m^h$ is isomorphic to $\mathcal{S}_n^k$ if and only if either $h=k$ and $m=n$ or $m+n=h+k=e$.*

PROOF. Assume that $m+n=h+k=e$. Then the map $\tau : (x,y) \mapsto (x, y^{2^n})$ on V is a bijective linear map which sends each point $(x, x^{2^m}t + xt^{2^h})$ of $X_m^h(t)$ to

$$(x, x^{2^{m+n}}t^{2^n} + x^{2^n}t^{2^{h+n}}) = (x, xt^{2^n} + x^{2^n}t^{2^{e-k+n}}) = (x, x^{2^n}t^{2^{n-k}} + x(t^{2^{n-k}})^{2^k}) \in X_n^k(t^{2^{n-k}}).$$

Thus τ gives a bijection of $\mathcal{S}_m^h$ with $\mathcal{S}_n^k$.

Conversely, assume that τ gives a bijection of $\mathcal{S}_m^h$ with $\mathcal{S}_n^k$. By Lemma 9, we may assume τ sends M_m^h to M_n^k. Denoting by X the matrix representing the multiplication by a generator ζ of $GF(q)^\times$, we may choose the following matrices as generators of M_m^h and M_n^k respectively:

$$\begin{pmatrix} X & 0 \\ 0 & X' \end{pmatrix} \text{ and } \begin{pmatrix} X & 0 \\ 0 & X'' \end{pmatrix}, \text{ where } X' := X^{(2^{m+h}-1)/(2^h-1)} \text{ and } X'' := X^{(2^{n+k}-1)/(2^k-1)}.$$

Since $\tau = \begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$, there is an index i with $0 \leq i \leq q-2$ such that $\tau^{-1}\begin{pmatrix} X & 0 \\ 0 & X' \end{pmatrix}\tau = \begin{pmatrix} X & 0 \\ 0 & X'' \end{pmatrix}^i$, that is, $A^{-1}XA = X^i$, $C^{-1}X'C = (X'')^i$ and $B(A^{-1}XA) = X'B$. The first equality shows that A normalizes the Singer cycle $\langle X \rangle$ of $GL_e(2)$, so that $A = X^j\sigma^a$ for some j and some field automorphism $\sigma^a : x \mapsto x^{2^a}$ of $GF(q)$. Then $i = 2^a$. Replacing τ by $\tau f_{(\sigma^a)^{-1}} m_\zeta^{-j}$, we may assume $a=0$ and $j=0$, that is, $A = I$.

Now the second equality is turned to $C^{-1}X'C = X''$. We will show that neither X' nor X'' lies in a subgroup of $\langle X \rangle$ corresponding to a proper nonprime subfield of $GF(q)$. Suppose, for example, X' is of order dividing 2^d-1 with a proper divisor d of e. We set $l := e/d > 1$ and $o(X') := (2^d-1)/\delta$ for some divisor δ of 2^d-1. The order of X' is also given by $(q-1)/(q-1, 2^{m+h}-1) = (q-1)/(2^f-1)$, where $f = (e, m+h)$, since the order of $X^{1/(2^h-1)}$ is the same as the order of X. Thus we have $\delta(2^{dl}-1) = \delta(q-1) = (2^d-1)(2^f-1)$, and $\delta(2^{d(l-1)} + \cdots + 2^d + 1) = 2^f - 1$. As $m+h \neq e$, $X' \neq 1$. Thus $d \geq 2$, and so $(2^{d(l-1)} + \cdots + 2^d + 1) > 2^{d(l-1)}$. In particular, $2^f - 1 > 2^{d(l-1)}$, and $f > d(l-1)$. As $m+h \neq e$, f is a proper divisor of e, and so $e/2 \geq f > d(l-1) = e-d$. Thus $d > e/2$, which is contrary to the assumption that d is a proper divisor of e. Hence X' and similarly X'' do not lie in a subgroup of $\langle X \rangle$ corresponding to a proper nonprime subfield of $GF(q)$. In particular, their centralizers in $GL_e(2)$ coincide with $\langle X \rangle$.

Then the equation $C^{-1}X'C = X''$ implies that C normalizes $\langle X \rangle$, and $C = X^j\sigma^a$ for some j and some field automorphism σ^a ($0 \leq a \leq e-1$). Thus we have

$$(*) \quad (X^{(2^{m+h}-1)/(2^h-1)})^{2^a} = X^{(2^{n+k}-1)/(2^k-1)}.$$

Moreover, for $x, y \in GF(q)$ we have

$$(x,y)\tau = (xA + yB, yC) = (x + yB, b \cdot y^{2^a}) \quad \text{with} \quad b := \zeta^{2^a j} \in GF(q)^\times.$$

Before examining the congruence among h, m, k, n obtained from $(*)$, we examine the third equality $B(A^{-1}XA) = X'B$ above. As $A = I$, we have $BX = X'B$. Now take a subspace $X = \{(0,y) | y \in GF(q)\}$ of $\mathcal{S}_m^h$, and consider its image $(X)\tau$ by τ. Since X is invariant under M_m^h and $(M_m^h)\tau = M_n^k$ by Lemma 9, the image $(X)\tau$ is also invariant under M_n^k. As $X \cap X_m^h(\alpha) = \{0\}$ for every $\alpha \in GF(q)$, $(X)\tau$ intersects trivially with every member of $\mathcal{S}_n^k$.

By Lemma 10, either $(X)\tau = \{(0, y) | y \in GF(q)\}$ or $(X)\tau = \{(x, cx^{\delta}) | x \in GF(q)\}$ for some $c \in GF(q)$, where $\delta := (2^{k+n} - 1)/(2^k - 1)$. Since $(0, y)\tau = (yB, by^{2^a})$, if the former case holds then $B = 0$.

Suppose the latter case occurs. Then B is a nonsingular matrix, for otherwise, $yB = 0$ for some $y \in GF(q)^{\times}$ but $(0, y)\tau = (yB, by^{2^a}) = (0, by^{2^a})$ is not of the form (x, cx^{δ}) for every $x \in GF(q)$. Thus $BXB^{-1} = X'$, and B normalizes the Singer cycle $\langle X \rangle$, and so $B = X^l \sigma^d$ for some l, d. Then $BXB^{-1} = X^{2^{-d}} = X' = X^{\delta}$ and so $X^{2^k - 1} = X^{2^d(2^{k+n}-1)}$. Thus $2^k + 2^d \equiv 2^{d+k+n} + 1 \pmod{2^e - 1}$. By [5, p.273, Chap. VIII, Lemma 4.4(c)], we have $\{k, d\} \equiv \{d + k + n, 0\} \pmod{e}$. As $k \not\equiv 0 \pmod{e}$, $k \equiv d + n + k$ and $d \equiv 0 \pmod{e}$, but this forces $n \equiv 0 \pmod{e}$, a contradiction. Hence the second case does not occur, and we always have $B = 0$. Thus we conclude

$$(**) \quad (x, y)\tau = (x, b \cdot y^{2^a}) \quad \text{for some} \quad b \in GF(q)^{\times} (x, y \in GF(q)).$$

Setting $\varepsilon := (2^h - 1)/(2^m - 1)$ and $\varepsilon' := (2^k - 1)/(2^n - 1)$, we have $X_m^h(0) \cap X_m^h(t) = (t^{\varepsilon}, 0)$ and $X_n^k(0) \cap X_n^k(t) = (t^{\varepsilon'}, 0)$. As $(t^{\varepsilon}, 0)\tau = (t^{\varepsilon}, 0) = ((t^{\varepsilon/\varepsilon'})^{\varepsilon'}, 0)$ by $(**)$, τ $(\in A)$ sends the unique member $X_m^h(t)$ of $\mathcal{S}_m^h - \{X_m^h(0)\}$ through $(t^{\varepsilon}, 0)$ to the unique member $X_n^k(t^{\varepsilon/\varepsilon'})$ of $\mathcal{S}_n^k - \{X_n^k(0)\}$ through $(t^{\varepsilon}, 0)\tau = (t^{\varepsilon}, 0)$. By $(**)$, $(X_m^h(t))\tau$ consists of $(x, x^{2^m} t + x t^{2^h})\tau = (x, b(x^{2^m} t + x t^{2^h})^{2^a})$ for $x \in GF(q)$. As they are contained in $X_n^k(t^{\varepsilon/\varepsilon'})$, we have

$$(***) \quad b(x^{2^m} t + x t^{2^h})^{2^a} = x^{2^n} t^{\varepsilon/\varepsilon'} + x(t^{\varepsilon/\varepsilon'})^{2^k} \text{ for every } x, t \in GF(q).$$

Putting $t = 1$ in $(***)$, we get $b(x^{2^m} + x)^{2^a} = x^{2^n} + x$ for every $x \in GF(q)$. This implies that the polynomial $f(\lambda) := b\lambda^{2^{a+m}} + b\lambda^{2^a} + \lambda^{2^n} + \lambda$ of $GF(q)[\lambda]$ of degree at most $2e - 2$ vanishes at every element of $GF(q)$, and hence it is a multiple of the minimal polynomial $\lambda^{2^e} + \lambda$.

If $a + m = e$, then $f(\lambda) = b(\lambda^{2^e} + \lambda)$, but this forces $n = 0$, a contradiction. Thus $a + m \neq e$ and $f(\lambda) = 0$, as $a, n < e$. Then we have $b = 1$ and $\{a + m, a\} \equiv \{n, 0\} \pmod{e}$, and therefore we conclude

$$\text{either (a) } m = n \text{ and } a = 0, \text{ or (b) } m + n = e \text{ and } a = n.$$

Finally we turn to equation $(*)$ above. Equation $(*)$ implies $(2^{m+h} - 1)2^a(2^k - 1) \equiv (2^{n+k} - 1)(2^h - 1) \pmod{2^e - 1}$, or equivalently

$$2^{a+m+h+k} + 2^{n+k} + 2^h + 2^a \equiv 2^{n+h+k} + 2^{a+m+h} + 2^{a+k} + 1 \pmod{2^e - 1}.$$

For case (a) of the conclusion in the above paragraph, we have $2^{m+h+k} + 2^{m+k} + 2^h + 1 \equiv 2^{m+h+k} + 2^{m+h} + 2^k + 1$, and so $2^m + 2^{h-k} \equiv 2^{m+h-k} + 1 \pmod{2^e - 1}$ from the above relation. By [5, p.273, Chap. VIII, Lemma 4.4(c)], we have $h = k$, as $m \not\equiv 0 \pmod{e}$. Thus in this case, we have $m = n$ and $k = h$. Similarly, for case (b), we have $2^{h+k} + 2^{n+k} + 2^h + 2^n \equiv 2^{n+h+k} + 2^h + 2^{n+k} + 1$ and so $2^{h+k} + 2^n \equiv 2^{n+h+k} + 1 \pmod{2^e - 1}$. Then $h + k = e$, as $n \not\equiv 0 \pmod{e}$. Hence $m + n = e$ and $h + k = e$ in this case. □

6. Some Functional Equations

Let A be the stabilizer of $X(0)$ in $Aut(\mathcal{S}_m^h)$ for the translation hyperoval $\mathcal{S}_m^h$. In Section 4, we determined A by exploiting group theory. To analyze the remaining smaller cases, we examine the functional equations determined by each automorphism of A. Since this approach is completely independent from the group theoretic one, every exposition in this section is stated as general as possible.

Let σ be an element of A. It determines maps $\xi = \xi(\sigma), \eta = \eta(\sigma) : V \to GF(q)$ ($W \to GF(q)$ if $m+h = e$) given by $(x, y)\sigma = (\xi(x, y), \eta(x, y))$. Since σ is a linear bijection on V (or W if $m+h = e$), we have $\xi(x+x', y+y') = \xi(x, y)+\xi(x', y')$ and $\eta(x+x', y+y') = \eta(x, y) + \eta(x', y')$ for $x, x', y, y' \in GF(q)$ (or $y, y' \in GF(q)_0$ if $m + h = e$). Then $\xi(x, y) = \xi_1(x) + \xi_2(y)$, where the maps $\xi_1(x) := \xi(x, 0)$ and $\xi_2(y) := \xi(0, y)$ are linear transformations on $GF(q)$. The map η is decomposed similarly, but $\eta_1(x) = \eta(x, 0) = 0$, as σ stabilizes $X(0) = \{(x, 0)|x \in GF(q)\}$. Thus $\eta(x, y) = \eta_2(y)$ is a linear transformation on $GF(q)$. For short we write $\eta(y) = \eta(x, y)$.

On the other hand, σ induces a permutation on the members of $\mathcal{S}_m^h$. Define a bijective map $f : GF(q) \to GF(q)$ by $(X(t))\sigma = X(f(t))$. We will express the linear transformations ξ_i ($i = 1, 2$) and η on V (or W if $m + h = e$) above in terms of f. For simplicity, we identify a projective point of $PG(V)$ with the unique nonzero vector in it.

Every point $(x, 0)$ of $X(0)$ is the intersection of $X(0)$ with $X(t)$, where $t^{(2^h-1)/(2^m-1)} = x$. As σ maps it to $(X(0))\sigma \cap (X(t))\sigma = X(0) \cap X(f(t)) = (f(t)^{(2^h-1)/(2^m-1)}, 0)$, we have

($d.\xi_1$)
$$\xi_1(t^{(2^h-1)/(2^m-1)}) = f(t)^{(2^h-1)/(2^m-1)} \qquad \text{for each } t \in GF(q).$$

The linearity of ξ_1 is equivalent to the following statement.

($l.\xi_1$) For $s, t \in GF(q)$, we have $f(s)^{(2^h-1)/(2^m-1)} + f(t)^{(2^h-1)/(2^m-1)} = f(u)^{(2^h-1)/(2^m-1)}$, where u is the element of $GF(q)$ uniquely determined from s and t by the equation $s^{(2^h-1)/(2^m-1)} + t^{(2^h-1)/(2^m-1)} = u^{(2^h-1)/(2^m-1)}$.

Choose any distinct elements s, t of $GF(q)^\times$. The intersection of $X(s)$ with $X(t)$ is

$$((s + t)^{(2^h-1)/(2^m-1)}, st(s^{2^h-1} + t^{2^h-1})(s + t)^{(2^h-2^m)/(2^m-1)}),$$

which is sent by σ to

$$X(f(s)) \cap X(f(t)) =$$
$$((f(s) + f(t))^{(2^h-1)/(2^m-1)}, f(s)f(t)(f(s)^{2^h-1} + f(t)^{2^h-1})(f(s) + f(t))^{(2^h-2^m)/(2^m-1)}).$$

The intersection $X(s + t) \cap X(0) = ((s + t)^{(2^h-1)/(2^m-1)}, 0)$ is mapped by σ to $X(f(s + t)) \cap X(0) = ((f(s+t)^{(2^h-1)/(2^m-1)}, 0)$. The third point of the line through $X(s) \cap X(t)$ and $X(s+t) \cap X(0)$ is $(0, y)$, where $y = st(s^{2^h-1}+t^{2^h-1})(s+t)^{(2^h-2^m)/(2^m-1)}$. This point is sent by σ to $(\xi_2(y), \eta(y))$, while it is also the third point on the line through $X(f(s)) \cap X(f(t))$ and $X(f(s + t)) \cap X(0)$. Thus for every $s, t \in GF(q)$ we have

$$\xi_2(st(s^{2^h-1} + t^{2^h-1})(s + t)^{(2^h-2^m)/(2^m-1)}) =$$
$$(f(s) + f(t))^{(2^h-1)/(2^m-1)} + f(s + t)^{(2^h-1)/(2^m-1)}, \quad \text{and}$$
$$\eta(st(s^{2^h-1} + t^{2^h-1})(s + t)^{(2^h-2^m)/(2^m-1)}) =$$
$$f(s)f(t)(f(s)^{2^h-1} + f(t)^{2^h-1})(f(s) + f(t))^{(2^h-2^m)/(2^m-1)}.$$

The above expressions give the functions ξ_2 and η over $GF(q)$ if $m + h \neq e$ (or $GF(q)_0$ if $m + h = e$) by Lemma 2. The well definedness of ξ_2 and η is equivalent to the following statement:

If $st(s^{2^h-1} + t^{2^h-1})(s + t)^{(2^h-2^m)/(2^m-1)} = s't'(s'^{2^h-1} + t'^{2^h-1})(s' + t')^{(2^h-2^m)/(2^m-1)}$ for $s, t, s', t' \in GF(q)$, then

$(d.\xi_2)$ $(f(s)+f(t))^{(2^h-1)/(2^m-1)}+f(s+t)^{(2^h-1)/(2^m-1)}=$
$(f(s')+f(t'))^{(2^h-1)/(2^m-1)}+f(s'+t')^{(2^h-1)/(2^m-1)}$,

$(d.\eta)$ $f(s)f(t)(f(s)^{2^h-1}+f(t)^{2^h-1})(f(s)+f(t))^{(2^h-2^m)/(2^m-1)}=$
$f(s')f(t')(f(s')^{2^h-1}+f(t')^{2^h-1})(f(s')+f(t'))^{(2^h-2^m)/(2^m-1)}$.

We do not give the explicit formulae for the linearity of ξ_2 and η, since they are complicated and not used later.

Summarizing, each element σ of A determines a bijective map f on $GF(q)$ with $f(0)=0$ which satisfies the above conditions $(d.\xi_i)$, $(d.\eta)$, $(l.\xi_1)$ and the linearity of ξ_2 and η.

Conversely, let f be a bijective map on $GF(q)$ with $f(0)=0$ satisfying these conditions. Define σ by $(x,y)\sigma=(\xi_1(x)+\xi_2(y),\eta(y))$, where

$$\xi_1(x)=f(u)^{(2^h-1)/(2^m-1)},\ \xi_2(y)=(f(s)+f(t))^{(2^h-1)/(2^m-1)}+f(s+t)^{(2^h-1)/(2^m-1)}$$
$$\text{and}\quad \eta(y)=f(s)f(t)(f(s)^{2^h-1}+f(t)^{2^h-1})(f(s)+f(t))^{(2^h-2^m)/(2^m-1)}$$
$$\text{for } s,t,u\in GF(q) \text{ with } x=u^{(2^h-1)/(2^m-1)},\ y=st(s^{2^h-1}+t^{2^h-1})(s+t)^{(2^h-2^m)/(2^m-1)}.$$

Clearly, ξ_1 is well defined and linear by $(l.\xi_1)$. By Lemma 2, the above formulae define ξ_2 and η on $GF(q)$ if $m+h\neq e$ (resp. on $GF(q)_0$ if $m+h=e$), which are well defined by $(d.\xi_2)$ and $(d.\eta)$. The linearity of ξ_2 and η on $GF(q)$ is assumed. Thus σ is a well defined linear map on V (or W if $m+h=e$) preserving $\mathcal{S}_m^h$. The map σ is bijective, since the function σ^{-1} similarly determined by f^{-1} gives the inverse map of σ. Hence σ lies in A.

The problem of finding the elements of A is now reduced to determine the bijective maps f on $GF(q)$ with the above conditions. Clearly, the multiplications and the field automorphisms of $\mathcal{S}_m^h$ satisfy those conditions. The problem is whether or not the other maps exist.

We introduce some notation. For a unordered pair $\{s,t\}$ of elements of $GF(q)$, $\nu(s,t)$ and $\mu(s,t)$ denote the elements of $GF(q)$ determined by

$$\nu(s,t)^{(2^h-1)/(2^m-1)}=s^{(2^h-1)/(2^m-1)}+t^{(2^h-1)/(2^m-1)},$$
$$\mu(s,t)=st(s^{2^h-1}+t^{2^h-1})(s+t)^{(2^h-2^m)/(2^m-1)}.$$

For $a\in GF(q)$, we denote by $\nu^{-1}(a)$ (resp. $\mu^{-1}(a)$) the set of pairs $\{s,t\}$ with $\nu(s,t)=a$ (resp. $\mu(s,t)=a$). Then the linearity of ξ_1 and the well definedness of η are equivalent to the following statements respectively

$(l.\xi_1)'$ f maps $\nu^{-1}(a)$ to $\nu^{-1}(f(a))$ for every $a\in GF(q)^\times$, and

$(d.\eta)'$ for every $a\in GF(q)^\times$, f maps $\mu^{-1}(a)$ to $\mu^{-1}(\eta(a))$, where $\eta(a)=\mu(f(s),f(t))$, which does not depend on the choice of $\{s,t\}\in\mu^{-1}(a)$.

Since f gives bijections of $\nu^{-1}(a)$ with $\nu^{-1}(f(a))$ and of $\mu^{-1}(a)$ with $\mu^{-1}(\eta(a))$ in the above, we have $|\nu^{-1}(a)|=|\nu^{-1}(f(a))|$ and $|\mu^{-1}(a)|=|\mu^{-1}(\eta(a))|$ for every $a\in GF(q)^\times$.

Note that if $h=1$ then $\mu(s,t)=st(s+t)^{1/(2^m-1)}$. If $m=h$, then $\xi_1=f$ and $\xi_2=0$, and hence we do not need the conditions for ξ_2.

7. Automorphism Groups for $e=3,4$

In this section, we will analyze the automorphism group $Aut(\mathcal{S}_m^h)$ for the case left remained in Lemmas 5 and 6. They are $\mathcal{S}_m^h$, $\{m,h\}\subseteq\{1,2\}$ for $e=3$ and $\mathcal{S}_m^h$, $\{m,h\}\subseteq\{1,3\}$ but $m+h\neq 4$ for $e=4$. By Propositions 8 and 11, we may assume that $(m,h)=(1,1)$ or $(2,1)$ if $e=3$, and $(m,h)=(1,1)$ if $e=4$. The dual hyperoval $\mathcal{S}_1^1$ is a 2 (resp.3)-dimensional dual

hyperoval in $PG(5,2)$ (resp. $PG(7,2)$) if $e=3$ (resp. $e=4$), while $\mathcal{S}_2^1$ is a 2-dimensional dual hyperoval in $PG(4,2)$ for $e=3$. We follow the notation in the previous section. As $h=1$, $\mu(s,t)=st(s+t)^{1/(2^m-1)}$. Let ζ be a generator of $GF(8)^\times$ (resp. $GF(16)^\times$) with $\zeta^3=\zeta+1$ (resp. $\zeta^4=\zeta+1$) if $e=3$ (resp. $e=4$).

LEMMA 12. *If $e=3$ and $m=h=1$, the map η is well defined and linear for every $GF(2)$-linear bijection f on $GF(8)$. Thus $Aut(\mathcal{S}_1^1)$ for $e=3$ is the split extension of $GF(8)$ by $GL_3(2)$.*

PROOF. As $m=h$, the conditions $(d.\xi_1)$ and $(l.\xi_1)$ are equivalent to the linearity of f and the conditions for ξ_2 are vacuous. Note the argument in the proof of Lemma 2 shows that for each $y\in GF(8)^\times$ the number of pairs of solutions $s,t\in GF(8)^\times$ of the equation $y=st(s+t)$ coincides with the number of elements $x\in GF(8)^\times$ with $Tr(y/x^3)=0$. As $\{x^3 | x\in GF(8)^\times\}=GF(8)^\times$, there are $(\frac{8}{2})-1=3$ pairs in $\mu^{-1}(y)$. They are $\{s,t\}$, $\{s,s+t\}$ and $\{t,s+t\}$ (trivial solutions), and hence $\eta(y)=f(s)f(t)f(s+t)$ is well defined. It remains to check the linearity of η.

The linear function f is uniquely determined by giving $(f(1),\ f(\zeta),\ f(\zeta^2))$. Let $(f_0,\ f_1,\ f_2)$ be any basis of $GF(8)$ over $GF(2)$, and let $f(1)=f_0$, $f(\zeta)=f_1$ and $f(\zeta^2)=f_2$. Then $f(a_0\cdot 1+a_1\cdot\zeta+a_2\cdot\zeta^2)=a_0f_0+a_1f_1+a_2f_2$ by the linearity of f. Now $h(y)$ can be explicitly given in terms of f_i $(i=0,1,2)$, consulting the following table, which is easy to verify. (It is enough to find one pair $\{s,t\}$ of $\mu^{-1}(y)$ for $y=1,\zeta,\zeta^3$, since the remaining two pairs of $\mu^{-1}(y)$ are $\{s,s+t\}$ and $\{t,s+t\}$, and the remaining $\mu^{-1}(y')$ $(y'\in GF(8)\setminus\{1,\zeta,\zeta^3\})$ are obtained by applying the field automorphisms in $Gal(8)$.)

x	$\mu^{-1}(x)$	x	$\mu^{-1}(x)$
1	$\{\zeta,\zeta^2\},\ \{\zeta,\zeta^4\},\ \{\zeta^2,\zeta^4\}$	ζ^4	$\{1,\zeta\},\ \{1,\zeta^3\},\ \{\zeta,\zeta^3\}$
ζ	$\{1,\zeta^2\},\ \{1,\zeta^6\},\ \{\zeta^2,\zeta^6\}$	ζ^5	$\{\zeta,\zeta^5\},\ \{\zeta,\zeta^6\},\ \{\zeta^5,\zeta^6\}$
ζ^2	$\{1,\zeta^4\},\ \{1,\zeta^5\},\ \{\zeta^4,\zeta^5\}$	ζ^6	$\{\zeta^3,\zeta^4\},\ \{\zeta^3,\zeta^6\},\ \{\zeta^4,\zeta^6\}$
ζ^3	$\{\zeta^2,\zeta^3\},\ \{\zeta^2,\zeta^5\},\ \{\zeta^3,\zeta^5\}$		

Using $\zeta^3=1+\zeta$, $\zeta^4=\zeta+\zeta^2$, $\zeta^5=1+\zeta+\zeta^2$ and $\zeta^6=1+\zeta^2$, we have:

$$
\begin{aligned}
\eta(1)&=f(\zeta)^2f(\zeta^2)+f(\zeta)f(\zeta^2)^2=f_1^2f_2+f_1f_2^2,\\
\eta(\zeta)&=f(1)^2f(\zeta^2)+f(1)f(\zeta^2)^2=f_0^2f_2+f_0f_2^2,\\
\eta(\zeta^2)&=f(1)^2f(\zeta^4)+f(1)f(\zeta^4)^2=f_0^2(f_1+f_2)+f_0(f_1+f_2)^2,\\
\eta(\zeta^3)&=f(\zeta^2)^2f(\zeta^3)+f(\zeta^2)f(\zeta^3)^2=f_2^2(f_0+f_1)+f_2(f_0+f_1)^2=\eta(1)+\eta(\zeta),\\
\eta(\zeta^4)&=f(1)^2f(\zeta)+f(1)f(\zeta)^2=f_0^2f_1+f_0f_1^2=\eta(\zeta)+\eta(\zeta^2),\\
\eta(\zeta^5)&=f(\zeta)^2f(\zeta^5)+f(\zeta)f(\zeta^5)^2=f_2^2(f_0+f_1+f_2)+f_2(f_0+f_1+f_2)^2\\
&=f_2^2(f_0+f_1)+f_2(f_0+f_1)^2=\eta(1)+\eta(\zeta)+\eta(\zeta^2),\\
\eta(\zeta^6)&=f(\zeta^3)^2f(\zeta^4)+f(\zeta^3)f(\zeta^4)^2=(f_0+f_1)^2(f_1+f_2)+(f_0+f_1)(f_1+f_2)^2\\
&=\eta(\zeta)+\eta(\zeta^2).
\end{aligned}
$$

Thus the linearity of η is verified for every choice of a basis $(f_0,\ f_1,\ f_2)$ of $GF(8)$ over $GF(2)$. Therefore, each linear bijective map $f\in GL(GF(8))\cong GL_3(2)$ gives an automorphism of $\mathcal{S}_1^1$ fixing the subspace $X(0)$. Thus $Aut(\mathcal{S}_1^1)$ is the split extension of the group of translation by $GL_3(2)$ with the natural action. □

LEMMA 13. *If $e=3$ and $m=2$, $h=1$, $Aut(\mathcal{S}_2^1)\cong A\Gamma L_1(8)\cong E_8:(Z_7:Z_3)$.*

PROOF. It is straightforward to verify the following tables, where $\mu^{-1}(y)$ is omitted if it is empty. We also omit the trivial member $\{0, \zeta^i\}$ of $\nu^{-1}(\zeta^i)$.

x	$\nu^{-1}(x)$	x	$\nu^{-1}(x)$
1	$\{\zeta, \zeta^5\}$, $\{\zeta^2, \zeta^3\}$, $\{\zeta^4, \zeta^6\}$	ζ^4	$\{1, \zeta^6\}$, $\{\zeta, \zeta^3\}$, $\{\zeta^2, \zeta^5\}$
ζ	$\{1, \zeta^5\}$, $\{\zeta^2, \zeta^6\}$, $\{\zeta^3, \zeta^4\}$	ζ^5	$\{1, \zeta\}$, $\{\zeta^2, \zeta^4\}$, $\{\zeta^3, \zeta^6\}$
ζ^2	$\{1, \zeta^3\}$, $\{\zeta, \zeta^6\}$, $\{\zeta^4, \zeta^5\}$	ζ^6	$\{1, \zeta^4\}$, $\{\zeta, \zeta^2\}$, $\{\zeta^3, \zeta^5\}$
ζ^3	$\{1, \zeta^2\}$, $\{\zeta, \zeta^4\}$, $\{\zeta^5, \zeta^6\}$		

y	$\mu^{-1}(y)$
ζ	$\{1, \zeta^3\}$, $\{1, \zeta^4\}$, $\{\zeta, \zeta^4\}$, $\{\zeta, \zeta^5\}$ $\{\zeta^2, \zeta^5\}$, $\{\zeta^2, \zeta^6\}$, $\{\zeta^3, \zeta^6\}$
ζ^2	$\{1, \zeta\}$, $\{1, \zeta^6\}$, $\{\zeta, \zeta^2\}$, $\{\zeta^2, \zeta^3\}$ $\{\zeta^3, \zeta^4\}$, $\{\zeta^4, \zeta^5\}$, $\{\zeta^5, \zeta^6\}$
ζ^4	$\{1, \zeta^2\}$, $\{1, \zeta^5\}$, $\{\zeta, \zeta^3\}$, $\{\zeta, \zeta^6\}$ $\{\zeta^2, \zeta^4\}$, $\{\zeta^3, \zeta^5\}$, $\{\zeta^4, \zeta^6\}$

Take any f with $f(0) = 0$ which satisfies the conditions $(l.\xi_1)'$ and $(d.\eta)'$. By composing a suitable multiplication, we may assume that $f(1) = 1$.

If $f(1) = 1$, we may assume that $f(\zeta) = \zeta$ or ζ^3, as field automorphisms fix 0 and 1. Assume $f(\zeta) = \zeta$. By $(l.\xi_1)'$, f permutes the three pairs of $\nu^{-1}(1)$. As $f(\zeta) = \zeta$, $\{f(\zeta), f(\zeta^5)\} = \{\zeta, \zeta^5\}$, and hence $f(\zeta^5) = \zeta^5$. By $(d.\eta)'$, f stabilizes $\mu^{-1}(\zeta)$ $(\ni \{\zeta, \zeta^5\})$ and $\mu^{-1}(\zeta^2)$ $(\ni \{1, \zeta\})$, and so $\mu^{-1}(\zeta^4)$. Observing the pairs of $\mu^{-1}(\zeta)$ containing 1, we have $\{f(\zeta^3), f(\zeta^4)\} = \{\zeta^3, \zeta^4\}$, and so $\{f(\zeta^2), f(\zeta^6)\} = \{\zeta^2, \zeta^6\}$. As $\mu^{-1}(\zeta^4)$ contains $\{1, \zeta^2\}$ but does not contain $\{1, \zeta^6\}$, we have $f(\zeta^i) = \zeta^i$ $(i = 2, 6)$. As $\mu^{-1}(\zeta^4)$ contains $\{\zeta, \zeta^3\}$ but does not $\{\zeta, \zeta^4\}$, we have $f(\zeta^i) = \zeta^i$ $(i = 3, 4)$. Hence f is the identity, and the original f lies in the semidirect product of the multiplications with the field automorphisms. When $f(\zeta) = \zeta^3$, a similar argument as above yields a contradiction. Thus $A = M : F$, and $Aut(\mathcal{S}_2) = T.A = T : (M : F) \cong A\Gamma L_1(8)$. □

LEMMA 14. *If $e = 4$ and $m = h = 1$, $Aut(\mathcal{S}_1^1) \cong A\Gamma L_1(16) \cong E_{16} : (Z_{15} : Z_4)$.*

PROOF. By Lemmas 5 and 6, it suffices to show that $A \ncong GL_4(2)$, where A is the stabilizer of $X(0)$ in $Aut(\mathcal{S}_1^1)$. As $m = h = 1$, $f = \xi_1, \xi_2 = 0$ and hence the well definedness of the function $\eta(y) = f(s) f(t) f(s + t)$ for $y = st(s + t)$ is the main property to check (see the proof of Lemma 12).

Assume that $A \cong GL_4(2)$. Then every linear bijection f on $GF(16)$ is induced by an automorphism σ of A. Choose a basis ζ^i $(i = 0, \ldots, 3)$ of $GF(16)$ over $GF(2)$ and set $f(\zeta^i) = f_i$ $(i = 0, \ldots, 3)$. It is straightforward to verify that $\mu^{-1}(\zeta)$ consists of:

$$\{1, \zeta^7\}, \{1, \zeta^9\}, \{\zeta^7, \zeta^9\};\ \{\zeta^2, \zeta^4\}, \{\zeta^2, \zeta^{10}\}, \{\zeta^4, \zeta^{10}\}; \{\zeta^5, \zeta^{12}\}, \{\zeta^5, \zeta^{14}\} \text{ and } \{\zeta^{12}, \zeta^{14}\}.$$

The well definedness of η on $y = \zeta$ implies that $f(1) f(\zeta^7) f(\zeta^9) = f(\zeta^2) f(\zeta^4) f(\zeta^{10})$. As $\zeta^7 = 1+\zeta+\zeta^3, \zeta^9 = \zeta+\zeta^3, \zeta^4 = 1+\zeta, \zeta^{10} = 1+\zeta+\zeta^2$, we have $f_0(f_0+f_1+f_3)(f_1+f_3) = f_2(f_0 + f_1)(f_0 + f_1 + f_2)$. Since f_3 appears in the left-hand side but not in the right-hand side, this is against the linear independency of f_i's. □

ACKNOWLEDGEMENTS

The author would like to express his hearty gratitude to Antonio Pasini for pointing out incompleteness included in the original version, and to William Kantor for his suggestion about the isomorphism problem.

REFERENCES

1. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and W. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.
2. B. Cooperstein and J. Thas, Communication through A. Pasini and A. Del Fra.
3. A. Del Fra, On d-dimensional dual hyperovals, preprint, June 1998.
4. C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces, preprint, 1998.
5. B. Huppert and N. Blackburn, *Finite Groups II*, Springer, 1982.
6. W. Kantor, Linear groups containing a Singer cycle, *J. Algebra*, **62** (1980), 232–234.
7. S. Yoshiara, A construction of extended generalized quadrangles using the Veronesean, *Europ. J. Combinatorics*, **18** (1997), 835–848.
8. S. Yoshiara, The universal cover of a family of extended generalized quadrangles, *Europ. J. Combinatorics*, **19** (1998), 753–765.

Received 26 October 1999 and accepted 7 April 1999

SATOSHI YOSHIARA
Division of Mathematical Sciences,
Osaka Kyoiku University,
Kashiwara,
Osaka 582,
Japan
E-mail: yoshiara@cc.osaka-kyoiku.ac.jp